Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Оценочные материалы по дисциплине

Социальная инженерия

по направлению подготовки

01.04.02 Прикладная математика и информатика

Направленность (профиль) подготовки:
Информационная безопасность

Форма обучения
Очная

Квалификация
Магистр

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
А.Ю. Матросова

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Компетенции и индикаторы их достижения, проверяемые данными оценочными материалами

Целью освоения дисциплины является формирование следующих компетенций:

ПК-2 Способен оценить уровень безопасности компьютерных систем и разработать программно-аппаратные средства защиты информации.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИПК-2.1 Осуществляет проведение контрольных проверок работоспособности и эффективности применяемых программно-аппаратных средств защиты информации, разработку требований к программно-аппаратным средствам защиты информации компьютерных систем.

ИПК-2.2 Осуществляет разработку требований по защите, формирование политик безопасности компьютерных систем и сетей, проектирование программно-аппаратных средств защиты информации компьютерных систем.

ИПК-2.3 Осуществляет проведение анализа безопасности компьютерных систем, проведение сертификации программно-аппаратных средств защиты информации и анализ результатов, разработку и тестирование средств защиты информации компьютерных систем.

2. Оценочные материалы текущего контроля и критерии оценивания

Элементы текущего контроля:
– теоретические вопросы;
– реферат;

Теоретические вопросы (ИПК-2.1, ИПК-2.3)

1. На вашу карту «по ошибке» пришли деньги от незнакомого человека. Указать основные опасности внезапного поступления денег.

Ответ:

Во-первых, нельзя забывать, что это не ваши средства. К вам может обратиться их владелец с просьбой вернуть деньги. Если оставить их себе, то на вас могут подать в суд и обвинить в присвоении чужих средств.

Перевести средства на вашу карту мог мошенник с целью использовать вас. Например, он может потребовать вернуть деньги и переслать их на другой счет и таким образом использовать вашу карту для отмывания денег.

Мошенники могут прибегнуть и к угрозам привлечения к гражданско-правовой и даже уголовной ответственности.

В таких схемах мошенники будут всеми силами торопить клиента совершить «транзакцию».

Мошенник может оставить номер вашей карты на фишинговом сайте или дать его человеку, который хочет что-то у него купить, не подозревая, что перед ним преступник.

Вы переведете деньги на другую карту, а обманутый человек будет считать вас мошенником и виноватым.

Мошенник может предложить вам «вернуть» ему часть денег. А себе оставить какую-то сумму за беспокойство. Это нужно, чтобы как-то вас убедить поучаствовать в его схеме, хотя вы этого не подозреваете.

Другой вариант: мошенник подделал СМС-ку и пересылает ее вам якобы от банка. А затем требует вернуть средства. Если вы не заметите подвоха, то на самом деле отправите ему свои деньги.

В планах у мошенника может быть и желание нажиться на вас. Он может попытаться выяснить секретные данные вашей карты, чтобы потом списать с нее ваши деньги.

Так что неожиданно пришедшие от незнакомца деньги – это далеко не повод для радости.

2. Что можно сделать, если на вашу карту «по ошибке» пришли деньги от незнакомого человека. Что делать, если вы оказались в такой ситуации?

Ответ:

Шаг 1. Не тратить деньги

Нужно запомнить, что тратить отправленные вам случайно деньги нельзя, как и переводить их на другой счет. Оставлять эти деньги ни в коем случае нельзя, потому что это уже будет нарушением закона. С вас могут потребовать возврата этих денег через суд. Если это какая-то мошенническая схема, то вас вообще могут счесть соучастником. А там уже может быть уголовное преследование.

Шаг 2. Проверить номер, с которого пришла СМС о переводе

Посмотрите на номер телефона, с которого пришла СМС. Мошенники могут прислать сообщение с любого мобильного номера и внутри подделать его текст, чтобы вам показалось, что оно пришло от банка.

Если номер кажется вам подозрительным и не совпадает с привычным номером банка, проверьте свой счет. На нем может не оказаться тех средств, которые якобы вам перевели. Отправленные на карту деньги иногда отображаются с опозданием, но все равно на это стоит обратить внимание.

Шаг 3. Обратиться в банк

Обратиться в ваш банк, рассказать о произошедшем и оставить заявку на возврат денежных средств на счет отправителя. Это можно сделать как по телефону, так и онлайн в чате с банком.

Критерии оценивания теста

Считается, что обучающийся успешно ответил на теоретические вопросы, если обучающийся при ответе демонстрирует знакомство с предметной областью и понимание сути проблемы, а ответ обучающегося содержит не менее половины правильных положений (утверждений) по сформулированному вопросу.

Реферат (ИПК-2.2)

Примеры тем рефератов

1. Принципы и техники социальной инженерии
2. Способы защиты от атак социальной инженерии
3. Утечка корпоративной информации и социальная инженерия
4. Психотипы и социальная инженерия
5. Методы социальной инженерии
6. Утечка информации в сети Интернет
7. Социальная инженерия в конкурентной разведке

8. Атаки с помощью социальных сетей
9. Фишинговые атаки.
10. Комбинированные схемы социальной инженерии
11. Ложные антивирусы
12. Лотереи
13. Троянские программы
14. Использование брендов известных фирм в организации атак
15. Техника претекстинга в социальной инженерии
16. Обратная социальная инженерия
17. Атаки с помощью сервиса FindFace
18. Анонимная сеть TOR
19. Способы получения корпоративной информации
20. Техническая разведка и её роль в организации атак СИ
21. Вредоносные программы в СИ
22. Службы разведки и СИ

Критерии оценивания реферата

Написание реферата преследует цель самостоятельного знакомства студентов с теоретической базой фундаментальных знаний по отдельным разделам социальной инженерии (по предложенной теме). Это позволит им в дальнейшем участвовать в творческом решении проблем информационной безопасности и научных подходов к организации безопасного использования современных информационно-телекоммуникационных технологий, содействовать реализации концепции устойчивого развития общества.

В процессе написания реферата студент должен решить следующие задачи:

1) Изучить проблемы по теме реферата с подбором литературы (источников).
2) Составить план реферата.
3) Обобщить собранный материал.
4) Написать реферат в соответствии с планом. В конце реферата сформулировать выводы, характеризующие отношение **автора реферата** к рассматриваемой проблеме и пути ее решения. Отправить реферат в текстовом формате на проверку. Ссылки на используемые источники в тексте реферата обязательны!
5) Подготовить доклад по теме реферата в виде файла в формате *.ppt.

Обязательные требования к написанию реферата:

- титульный лист с названием темы
- аннотация
- оглавление (содержание)
- текст реферата с указанием ссылок на цитируемые источники
- выводы
- список литературы, включая ссылки на адреса веб-сайтов с цитируемыми материалами.

При выполнении всех требований реферат оценивается **«зачтено»**. В случае плагиата (копировании чужой работы) – «**не зачтено»** и студент получает у преподавателя новую тему.

3. Оценочные материалы итогового контроля (промежуточной аттестации) и критерии оценивания

Изучение курса завершается сдачей зачёта. Зачёт ставится при положительных результатах текущего контроля, положительных ответах на вопросы билета и сдаче реферата и доклада по одной из предложенных преподавателем тем. Методические

материалы и требования к реферату включают критерии оценивания теоретических вопросов; процедуру формирования итоговой оценки, учитывающую оценки за каждую компетенцию.

Процедура формирования итоговой оценки включает степень самостоятельности студента при знакомстве с теоретической базой фундаментальных знаний по отдельным разделам социальной инженерии (по предложенной теме), полноту раскрытия темы, уровень обобщения собранного материала и отношение автора реферата к рассматриваемой проблеме и путям её решения.

4. Оценочные материалы для проверки остаточных знаний (сформированности компетенций)

Теоретические вопросы (ИПК-2.2):

1. Основные проблемы инженерно-технической защиты информации.
2. Виды информации, подлежащие защите. Государственная тайна.
3. Принципы и техники социальной инженерии.
4. Способы защиты от атак социальной инженерии.
5. Утечка корпоративной информации и социальная инженерия.
6. Психические состояния и социальная инженерия.
7. Методы социальной инженерии.
8. Утечка информации через Интернет.
9. Социальная инженерия в конкурентной разведке.
10. Социальная инженерия. Техника претекстинг.
11. Социальная инженерия Использование брендов известных фирм.
12. Социальная инженерия. Лотереи.
13. Социальная инженерия. Ложные антивирусы.

Информация о разработчиках

Беляев Виктор Афанасьевич, канд. техн. наук, доцент кафедры компьютерной безопасности института прикладной математики и компьютерных наук НИ ТГУ.